

The Challenge of Implementing the NERC CIP Cyber Security Standard

2006 International Control
Systems Security and Standards
Coordination Workshop

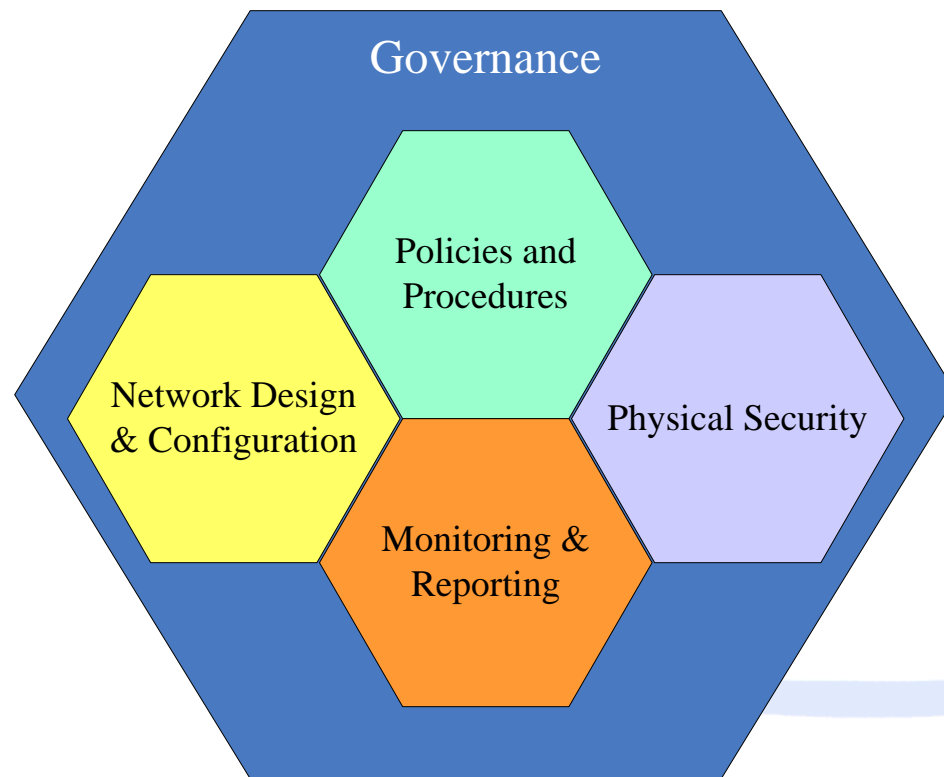
Portland
August 10–11



Key Questions:

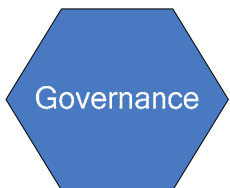
- How complicated can it really be to **establish** an effective security program?
- What type of **organizational issues** need to be addressed:
 - Who needs to be involved?
 - Who should be in charge?
 - Who will maintain the security program?
- What are the major **technical** issues?
- What are the major **cultural** issues?
- How much of an **effort** will be required?
- What are the **benefits**?

Key Security Program Ingredients



Key Security Program Ingredients

- Corporate **governance** framework;
 - Complex organizations will require broad corporate visibility (not just operations);
 - Sr. management accountability and responsibility for:
 - Design
 - Implementation
 - Operations and Maintenance
 - Physical and cyber security organizational;
 - Integration with existing security programs for business networks and other infrastructures.

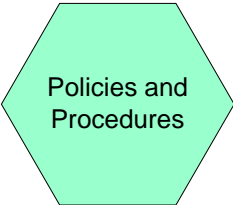


Key Security Program Ingredients

- **Network design and configuration;**
 - Without a security-centric network design and configuration, all the policies and procedures in the world will not make the facilities secure;
 - Establish design and configuration standards (ISO / NERC / NIST);
 - Electronic security perimeter design for critical cyber assets;
 - Impacts implementation costs of program
 - Impacts operational costs of program.

Key Security Program Ingredients

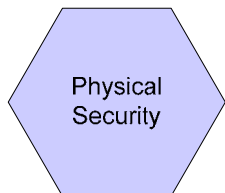
- **Policies and procedures** that are complimentary and commensurate with:
 - Appropriate Standards;
 - Governance provisions;
 - Responsible entity critical success factors (CSF's).



Policies and
Procedures

Key Security Program Ingredients

- **Physical security** that protects critical cyber assets and critical assets commensurate with:
 - Appropriate Standards
 - Electronic security perimeter;
 - Responsible entity critical success factors (CSF's)



Key Security Program Ingredients

- Effective compliance **monitoring and reporting** / Audit Proof
 - Review of policies and procedures to ensure compliance with applicable standards;
 - Review of actual practices to ensure they are consistent with the established policies and procedures;
 - Effective controls are in place.



How complicated are the standards?

NERC CIP CYBER SECURITY STANDARDS Eight Standards / 41 Requirements

CIP-002

CRITICAL CYBER ASSETS

1. CRITICAL ASSETS
2. CRITICAL CYBER ASSETS
3. ANNUAL REVIEW
4. ANNUAL APPROVAL

CIP-003

SECURITY MANAGEMENT CONTROLS

1. CYBER SECURITY POLICY
2. LEADERSHIP
3. EXCEPTIONS
4. INFORMATION PROTECTION
5. ACCESS CONTROL
6. CHANGE CONTROL

CIP-004

PERSONNEL AND TRAINING

1. AWARENESS
2. TRAINING
3. PERSONNEL RISK ASSESSMENT
4. ACCESS

CIP-005

ELECTRONIC SECURITY

1. ELECTRONIC SECURITY PERIMETER
2. ELECTRONIC ACCESS CONTROLS
3. MONITORING ELECTRONIC ACCESS
4. CYBER VULNERABILITY ASSESSMENT
5. DOCUMENTATION

CIP-006

PHYSICAL SECURITY

1. PLAN
2. PHYSICAL ACCESS CONTROLS
3. MONITORING PHYSICAL ACCESS
4. LOGGING PHYSICAL ACCESS
5. ACCESS LOG RETENTION
6. MAINTENANCE & TESTING

CIP-007

SYSTEMS SECURITY MANAGEMENT

1. TEST PROCEDURES
2. PORTS & SERVICES
3. SECURITY PATCH MANAGEMENT
4. MALICIOUS SOFTWARE PREVENTION
5. ACCOUNT MANAGEMENT
6. SECURITY STATUS MONITORING
7. DISPOSAL OR REDEPLOYMENT
8. CYBER VULNERABILITY ASSESSMENT
9. DOCUMENTATION

CIP-008

INCIDENT REPORTING & RESPONSE PLANNING

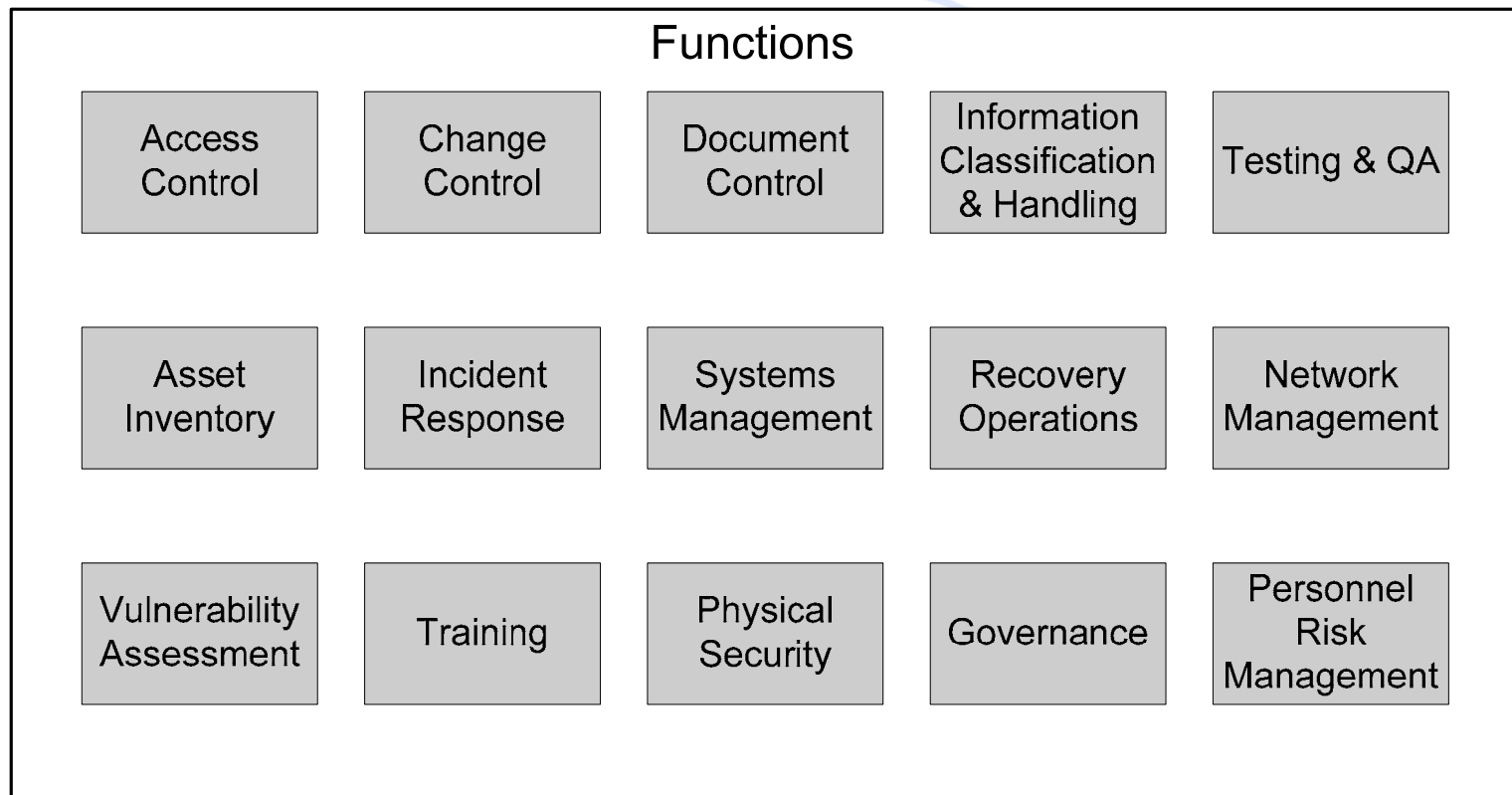
1. CYBER SECURITY INCIDENT RESPONSE PLAN
2. DOCUMENTATION

CIP-009

RECOVERY PLANS FOR CCA

1. RECOVERY PLANS
2. EXERCISES
3. CHANGE CONTROL
4. BACKUP & RESTORE
5. TESTING BACKUP MEDIA

Security Program Functional Framework



Benefits of Functional Framework

- Simplifies security program processes for:
 - Development
 - Implementation
 - On going operations and maintenance
- Provides a framework for training and security awareness

Security Program Functional Framework

Function / Standard Requirements Matrix

Function	CIP-002 Critical Cyber Asset Identification	CIP-003 Security Management Controls	CIP-004 Personnel and Training	CIP-005 Electronic Security Perimeters	CIP-006 Physical Security	CIP-007 Systems Security Management	CIP-008 Incident Reporting and Response Planning	CIP-009 Recovery Plans for Critical Cyber Assets
Asset Inventory	R1-R4					R7		
Network Management		R6		R1				
Change Management		R5 R1/R2/R3	R4	R2/R3		R5		
Access Control							R1/R2	
Governance								
Incident Response								
Inform Class		R4						
Document Control	All	All	All	All	All	All	All	All
Personnel Risk Assess			R3					
Physical Security					R1-R6			
Recovery Operations								R1-R5
Systems Mgmt						R2/R3/R4/R6		
Testing						R1		
Training			R1/R2					
Vul Assessmwent				R4/R5		R8/R9		

Typical Organizational Impact Matrix

	<div>ORGANIZATION</div> <div>FUNCTION</div>	IT Management Services	Facilities Security	Grid Operations	Substation Engineering	Energy Supply	Human Resources	Audit Services	General Counsel	Corporate Communications	Vendors
1	Access Control	X	X	X	X	X	X				X
2	Change Management	X		X	X	X	X				X
3	Document Control	X	X	X	X	X			X		X
4	Information Classification & Handling	X	X	X	X	X	X	X	X	X	X
5	Testing & Q/A			X	X	X					X
6	Asset Inventory Management		X	X	X	X					
7	Vulnerability Assessment	X	X	X	X	X		X			
8	Incident Response	X	X	X	X	X			X	X	X
9	Systems Management	X		X	X	X					X
10	Training	X	X	X	X	X	X			X	X
11	Physical Security		X	X	X	X					X
12	Recovery Operations	X	X	X	X	X				X	X
13	Governance	X	X	X	X	X	X	X	X	X	
14	Personnel Risk Management		X	X	X	X	X		X		
15	Network Management	X		X	X	X					X

Organizational Issues:

- HR may be involved in employee “personnel risk assessment”, validation of employee status, and training;
- General Counsel / Legal / Contracts are typically involved in agreements and provisions for contractors and vendors who work on the critical assets;
- Corporate IT may retain some responsibilities in network management, access point controls, and communications;

ORGANIZATION		IT Management Services	Facilities Security	Grid Operations	Substation Engineering	Energy Supply	Human Resources	Audit Services	General Counsel	Corporate Communications	Vendors
FUNCTION											
1	Access Control	X	X	X	X	X	X				X
2	Change Management	X		X	X	X	X				X
3	Document Control	X	X	X	X	X			X		X
4	Information Classification & Handling	X	X	X	X	X	X	X	X	X	X
5	Testing & Q/A			X	X	X					X
6	Asset Inventory Management		X	X	X	X					
7	Vulnerability Assessment	X	X	X	X	X		X			
8	Incident Response	X	X	X	X	X			X	X	X
9	Systems Management	X		X	X	X					X
10	Training	X	X	X	X	X	X			X	X
11	Physical Security		X	X	X	X					X
12	Recovery Operations	X	X	X	X	X				X	X
13	Governance	X	X	X	X	X	X	X	X	X	
14	Personnel Risk Management		X	X	X	X	X		X		
15	Network Management	X		X	X	X					X

Organizational Issues:

- Substation engineering – substation automation, power quality, pilot protection, and incident analysis of substation operations;
- Energy supply – reliability of the bulk electric systems, key substations, black start plants.

ORGANIZATION		IT Management Services	Facilities Security	Grid Operations	Substation Engineering	Energy Supply	Human Resources	Audit Services	General Counsel	Corporate Communications	Vendors
FUNCTION											
1	Access Control	X	X	X	X	X	X				X
2	Change Management	X		X	X	X	X				X
3	Document Control	X	X	X	X	X			X		X
4	Information Classification & Handling	X	X	X	X	X	X	X	X	X	X
5	Testing & Q/A			X	X	X					X
6	Asset Inventory Management		X	X	X	X					
7	Vulnerability Assessment	X	X	X	X	X		X			
8	Incident Response	X	X	X	X	X			X	X	X
9	Systems Management	X		X	X	X					X
10	Training	X	X	X	X	X	X			X	X
11	Physical Security		X	X	X	X					X
12	Recovery Operations	X	X	X	X	X				X	X
13	Governance	X	X	X	X	X	X	X	X	X	
14	Personnel Risk Management		X	X	X	X	X		X		
15	Network Management	X		X	X	X					X

Organizational Issues:

- Internal audit will become more and more involved in validating the effectiveness of internal controls through SAS 70 and SOX audits;
- External entities (such as contractors, vendors, customers) will need access to various assets

	ORGANIZATION FUNCTION										
		IT Management Services	Facilities Security	Grid Operations	Substation Engineering	Energy Supply	Human Resources	Audit Services	General Counsel	Corporate Communications	Vendors
1	Access Control	X	X	X	X	X	X				X
2	Change Management	X		X	X	X	X				X
3	Document Control	X	X	X	X	X			X		X
4	Information Classification & Handling	X	X	X	X	X	X	X	X	X	X
5	Testing & Q/A			X	X	X					X
6	Asset Inventory Management		X	X	X	X					
7	Vulnerability Assessment	X	X	X	X	X		X			
8	Incident Response	X	X	X	X	X			X	X	X
9	Systems Management	X		X	X	X					X
10	Training	X	X	X	X	X	X			X	X
11	Physical Security		X	X	X	X					X
12	Recovery Operations	X	X	X	X	X				X	X
13	Governance	X	X	X	X	X	X	X	X	X	
14	Personnel Risk Management		X	X	X	X	X		X		
15	Network Management	X		X	X	X					X

Technical Issues:

- Configuration Management
 - Configuration management is paramount in the ongoing **asset management, access control, and change control** functions for an effective security program.
 - Configuration control needs to address the identity of:
 - Critical assets;
 - Critical cyber assets, ports, services, etc.
 - Access points;
 - Inter-relationships of critical cyber assets;
 - People who have access to critical cyber assets.
 - Configuration management structures will require adjustments for various asset types and operating characteristics.

Technical Issues:

- Access Control
 - Who has access to what?
 - Access control involves **people, assets, and authentication processes** here-to-for not typically addressed in identity management or similar programs;
 - How is access provisioned and de-provisioned?
 - Assurance that synchronization is maintained between **authorized** and **actual** access provisioning / de-provisioning will be required and audited.

Technical Issues:

- Document Control;
 - Infrastructure configurations;
 - Network design;
 - Floor plans of critical facilities;
 - Incident response and recovery plans;
 - Testing results;
 - Asset information.
- Operational Efficiency
 - Leverage technology through process automation and effective controls;
 - Keep it simple
 - Manage level of detail

Cultural Issues:

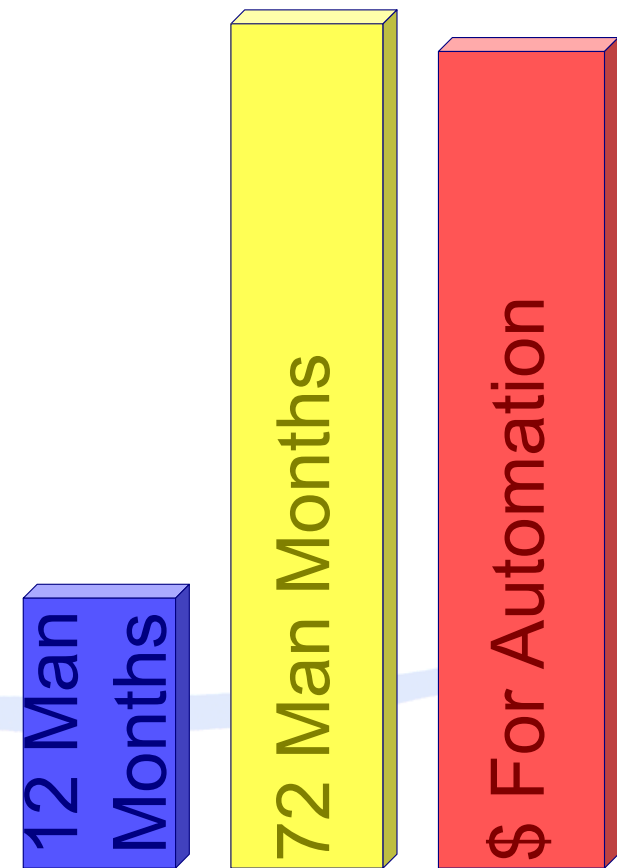
- Implementation of “New” Processes;
 - Access control granulation
 - Password management
 - Change management
 - Configuration management
 - Document management
 - Event monitoring and documentation
 - Software design
 - Testing
- Organizational Responsibilities
 - Turf battles
 - Collaborative processes

Key Deliverables:

- Policy & procedures (estimates);
 - 20 Policies
 - 40 Procedures
 - 70 Documents (Reports, Logs, Drawings)
- Network design & configuration evaluation;
- Physical security initiatives;
- Organization restructuring;
- Training program.

Level of Effort Attributes

- Size, complexity, and nature of organization;
- Number and location of **critical cyber assets**;
- Established provisions for **physical security** of critical cyber assets;
- Current **cyber security provisions** of networked infrastructures and access control points within electronic security boundaries;
- **Compliance** of existing policies and procedures with standard;
- Availability of required technical **support systems**.



Benefits

- Enhanced **reliability** and availability of the bulk electric system;
- Improved incident **response**;
- Improved **audit** reporting;
- **Optimized utilization** of resources through the implementation of **risk** management concepts and **alignment** with CSFs;
- **Investment** in operational **resiliency**.

